WHAT IS CLAIMED IS:

1. A second storage comprising:

a plurality of nonvolatile data storing means;

a controller of the nonvolatile data storing means; and

an internal network for interconnecting the nonvolatile data storing means with the controller,

wherein the controller comprises a plurality of network transportation ports connected to different networks, respectively, an access controller for processing I/O commands requested for the transportation ports, and an access controlling table for storing access control setting information which defines the I/O commands to be authorized between one of the plurality of transportation ports and one of the plurality of nonvolatile data storing means.

2. A second storage according to claim 1, wherein the access controller judges the authorization or rejection of the I/O commands requested for the transportation ports based on the access control setting information.

3. A second storage according to claim 1, wherein the access control setting information is set to the I/O commands to be authorized between a logical disk to be set

to the plurality of nonvolatile data storing means and one of the plurality of transportation ports.

4. A second storage according to claim 1, comprising a management console for setting and changing the access control setting information.

5. A second storage according to claim 1, containing access control setting information which is set as readout unauthorized with respect to all the transportation ports.

6. A second storage according to claim 3, wherein the access controller reports the I/O command judged as unauthorized to the management console.

7. A second storage according to claim 5, wherein the management console comprises record means for recording the I/O commands reported from the access controller.

8. An access controlling method of a second storage, comprising:

a controller having a plurality of network ports connected to different networks, respectively, an access controller for processing I/O command requested for the network ports, and an access controlling table for storing access control setting information which defines the I/O commands to be authorized between one of the plurality of network ports and one of the plurality of nonvolatile data storing means;

a plurality of nonvolatile data storing means; and

an internal network for interconnecting the nonvolatile data storing means with the controller, wherein the access controller

extracts an identifier of a data targeted by the I/O command from the I/O command received at the network port,

confirms a nonvolatile data storing means to which the data will be read or stored, the network port that received the I/O command,

refers to the access controlling table, and

judges whether or not the I/O command is authorized between the network port and the nonvolatile data storing means.

10. An access controlling method according to claim 8, wherein when a judgment frequency of the access non-authorization to specific data stored in the nonvolatile data storing means exceeds a predetermined threshold, access from the plurality of transportation ports to the data is not authorized.

11. An access controlling method according to claim 8, wherein when a judgment frequency of the access

non-authorization to specific data stored in the nonvolatile data storing means exceeds a predetermined threshold, an administrator of the second storage is notified that the judgment frequency of the access non-authorization exceeds a predetermined threshold.

12. An access controlling method according to claim 8, wherein when a system of the I/O commands is the SCSI (Small Computer System Interface) standards, a "CHECK CONDITION" status is transmitted as a report of abnormalities.

13. An access controlling method according to claim 12, wherein when a "REQUEST SENSE" request is issued after a host computer received the "CHECK CONDITION" status, a code denoting abnormalities is transmitted as a sense key and sense data in response thereto.

14. An access controlling method according to claim 13, wherein an "Illegal Request" is transmitted as the sense key.

15. An access controlling method according to claim 13, wherein "Data Protected" is transmitted as the sense key.

16. An access controlling method according to claim 8, wherein when a system of the I/O commands is NFS (Network File System), a NFS error code "NFSERR_PERM" is transmitted as a report of the access non-authorization.

17. An access controlling method according to claim 8, wherein when a system of the I/O commands is NFS (Network File System), a NFS error code "NFSERR_ACCS" is transmitted as a report of the access non-authorization.